AN A.S. PRATT PUBLICATION
SEPTEMBER 2016
VOL. 2 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 NUMBER 7 SEPTEMBER 2016

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [227] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Circuit Courts and FTC Take on Definitions of "PII" While Michigan Amends Privacy Law to Remove Statutory Damages – Part I

By Christin S. McMeley and John D. Seiver*

In this two-part article, the authors discuss the implications of recent developments regarding the definition of "personally identifiable information" ("PII"). This first part of the article explains recent court decisions on the issue and discusses the evolving definitions of "PII" and "Consumer" under the Video Privacy Protection Act. The second part of the article, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report*, will examine the Federal Trade Commission's interpretation of what constitutes PII, Michigan's amendments to its Video Rental Privacy Act, and the impact of these developments on content providers.*

The U.S. Court of Appeals for the First Circuit recently handed down its widely anticipated opinion in *Yershov v. Gannett Satellite Information Network, Inc.*,[1] in which it expanded the reach of the Video Privacy Protection Act[2] ("VPPA" or "Act") by endorsing a view of how the statute applies in the digital media context that was seen as more expansive than the holdings of other courts. In its decision, the court held that (1) "personally identifiable information" ("PII") includes the GPS coordinates of a device; and (2) a user of a mobile application – even one who does not pay or otherwise register to use the app – qualifies as a "consumer" entitled to the protections of the Act. Accordingly, Gannett's sharing of the GPS coordinates of a device used to access videos on the USA Today website, along with the titles of the videos, constituted a violation of the VPPA.

However, in a subsequent decision, *In Re Nickelodeon*,[3] the U.S. Court of Appeals for the Third Circuit dismissed VPPA claims based on the sharing of video titles viewed, along with non-GPS information about the viewer, such as IP addresses and persistent identifiers found in online advertising cookies. The Third Circuit stated that it did not see a conflict with *Yershov* because "GPS coordinates contain

* Christin S. McMeley, a partner at Davis Wright Tremaine LLP and chair of the firm's Privacy & Security Practice, advises companies in privacy compliance, information governance, data security, public policy, and regulatory matters. John D. Seiver, of counsel at the firm, practices communications and privacy law, representing cable television, internet, technology, and telecommunications companies. The authors may be reached at christinmcmeley@dwt.com and johnseiver@dwt.com, respectively.

[1] http://media.ca1.uscourts.gov/pdf.opinions/15-1719P-01A.pdf.

[2] https://www.gpo.gov/fdsys/pkg/USCODE-2014-title18/html/USCODE-2014-title18-partI-chap121-sec2710.htm.

[3] http://www2.ca3.uscourts.gov/opinarch/151441p.pdf.

more power to identify a *specific person* than, in our view, an IP address, a device identifier, or a browser fingerprint." The Third Circuit went on to hold that the definition of PII under the VPPA is not "so broad as to cover the kinds of static digital identifiers at issue here" when such identifiers cannot be associated with "a particular person's video-watching habits" by an "ordinary recipient" with "little or no extra effort." The court found that because it was necessary to engage in "detective work" to connect an actual person to the *identifiers* that disclosed the videos watched meant that PII was not improperly shared.

The defendants in *Nickelodeon* did not challenge whether visitors to Viacom's website were "consumers" entitled to VPPA protection, but the defendants in *Yershov* did. Although the defendants in *Yershov* prevailed in the district court, the First Circuit reversed and significantly expanded most other courts' limited interpretation of "consumers" entitled to the protection of the Act. Those decisions (including one that relied on the now-reversed district court decision in *Yershov*) have generally held there must be some ongoing commitment by the consumer, even if the commitment was not monetary, beyond merely downloading an app or using a service. The First Circuit acknowledged that there were issues of fact not considered on a motion to dismiss such that, after remand and discovery, the district court could still find that Yershov was not a "subscriber" and that Gannett did not violate the VPPA.

Plaintiffs in any circuit may be encouraged by a Federal Trade Commission ("FTC") blog entry[4] posted by Director Jessica Rich on April 21, in which she stated that the FTC "regard[s] data as 'personally identifiable,' and thus warranting privacy protections, when it can be *reasonably linked* to a particular person, computer, or device" (emphasis in original). Director Rich went on to state that "in many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test." The contours of how easy or difficult it should be to "link" an identifier in order to qualify as PII under the VPPA will continue to be a hotly contested issue in pending and future cases, especially since the *Nickelodeon* decision generally comes out the other way on device identifiers.

Moreover, as information proliferates and the definitions of PII and "personal information" evolve, legacy statutes enacted in brick-and-mortar world present more risk in today's digital environment, especially when statutory damages are involved. To address this problem, Michigan recently amended its state version of the VPPA to both (1) eliminate the $5,000 per person statutory damage provision and require *actual damages* as a result of an alleged violation; and (2) permit the disclosure of PII in the ordinary course of business, *including when marketing goods and services to customers or potential customers*, when advance written notice is provided.

---

[5] https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry?utm_source=govdelivery.

While the Michigan amendments are an important development for a number of publishers that have been targeted in state class actions, they provide no relief under the federal VPPA, nor are we likely to see similar amendments at the federal level in the near future. Congress amended the VPPA once recently to accommodate Netflix, and it is unlikely they will relax any of its provisions. Therefore, as this body of case law develops, it is important for companies who disclose consumer viewing data coupled with other identifiers to consider approaches that reduce the plausible "linkage" between such identifiers and a person's actual identity.

EVOLVING DEFINITIONS OF "PII" AND "CONSUMER" UNDER THE VPPA

The VPPA prohibits the "knowing" disclosure of "personally identifiable information" of a "consumer of such provider" except in narrow and clearly defined circumstances. The two central issues considered by the court in *Yershov* were whether the information shared constituted PII, and whether the plaintiff was a "consumer" for purposes of the statute. Yershov alleged that Gannett violated the VPPA by sharing with Adobe data related to the videos he viewed through its free USA Today Mobile App which consisted of: (1) the title of the video viewed; (2) the GPS coordinates of the device at the time the video was viewed; and (3) unique device identifiers.

The court, taking the pleaded allegations as true, found that Adobe was able to combine the information provided by Gannett with a larger profile of information about the plaintiff gathered from other sources, in order to personally identify him and the videos he was watching (thus triggering the potential VPPA violation). According to the court:

> [W]hen a football referee announces a violation by 'No. 12 on the offense,' everyone with a game program knows the name of the player who was flagged. . . . [A]ccording to the complaint, when Gannett makes such a disclosure to Adobe, it knows that Adobe has the 'game program,' so to speak, allowing it to link the GPS address and device identifier information to a certain person by name, address, phone number, and more.

The court did recognize that "there is certainly a point at which the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work," but concluded that in this case "the linkage, as plausibly alleged, is both firm and readily foreseeable to Gannett." The court found that GPS coordinates are more like a traditional street address than numeric device IDs such that their disclosure "effectively reveal[ed] the name of the video viewer."

Because the First Circuit on review of a motion to dismiss had to accept the allegations as true, it remanded for further proceedings, where Defendants may argue that even precise location information does not identify a person, but merely a location where hundreds of other people may be gathered or associated with the particular device. The evidence on remand will ultimately prove or disprove what Gannett actually knew or what was reasonably foreseeable, and thus whether the linkage was enough to constitute a violation of the VPPA. Although the information Gannett transferred to a third party also included unique device identifiers (*i.e.*, an Android ID), the court noted that its holding "need not be quite as broad as [its] reasoning suggests," leaving unanswered the question of whether device identifiers alone would constitute PII.

With this condition set out in the holding, the decision may not be as far out of step with a slew of prior federal district court decisions holding that a consumer's personal data, when disclosed, must identify a particular individual, *without more*, to qualify as PII. While *Yershov* appeared to hinge on the transmission of GPS coordinates, the Third Circuit in *Nickelodeon* addressed persistent identifiers directly, and found that most device identifiers are too remote to be considered PII. Finding it unadvisable to craft a "single-sentence holding capable of mechanistically deciding future cases" regarding the definition of "personally identifiable information," the court in *Nickelodeon* went on to "articulate a more general framework" for determining what information constitutes PII for purposes of the VPPA. In doing so, the court held that "personally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior." The court was quick to point out that this framework does not conflict with the *Yershov* decision, and that changes in technology or other factual circumstances could result in a numeric identifier qualifying as PII (giving nod to the identifier that could be tied to a registered user's Facebook account in the *Hulu* case).

However, in today's world, IP addresses and many other persistent identifiers cannot, by themselves, be tied to a particular person, so could not be PII under the VPPA. For instance, Internet Service Providers maintain logs of IP addresses that can be later correlated to subscribers through other secure systems. Certain websites require registration and rely on persistent identifiers from cookies. In both cases, that tying information (the IP logs, billing systems, or the registration IDs) is not available to the public. Indeed, as the First Circuit noted, there has been considerable copyright litigation where plaintiff copyright owners or their agents seek the identity of allegedly infringing individuals by suing "John Does" identified only by an IP address. Plaintiffs subsequently learn the identity of the individual by serving a subpoena and obtaining a court order that requires the ISP to disclose which subscriber used that IP address, and that disclosure must comply with additional privacy laws. The need for subpoenas and court orders to unearth the household (not even necessarily the actual user) where the

internet traffic travelled to and from clearly indicates that significant "detective work" must be done to use IP addresses to identify any specific person.

In addition to addressing the question of PII, the First Circuit also considered whether Yershov qualified as a "consumer" entitled to the VPPA's protections. The VPPA defines a consumer as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." The court easily ruled out Yershov as a renter or purchaser, but held that Yershov was a Gannett "subscriber."

In a decision that was relied on by the U.S. Court of Appeals for the Eleventh Circuit in *Ellis v. Cartoon Network, Inc.*, the district court had found that Yershov was not a "subscriber" because he did not have to pay, register, or make any commitments to use the App to access the USA Today videos. In reversing the district court, the First Circuit found instead that the plaintiff was a subscriber because "[t]o use the App, Yershov did indeed have to provide Gannett with personal information, such as his Android ID and his mobile device's GPS location at the time he viewed a video, each linked to his viewing selections. While he paid no money, access was not free of a commitment to provide consideration in the form of that information, which was of value to Gannett."

***

The second part of this article will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report.*